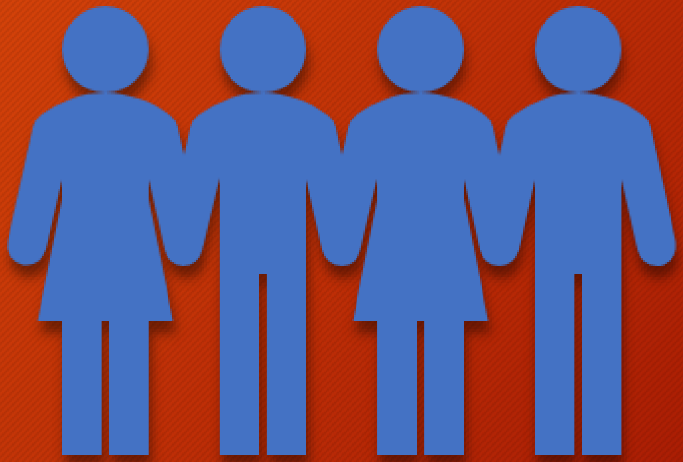
Cybersecurity for Emergency Managers

Alaska Spring
Preparedness Conference
2019

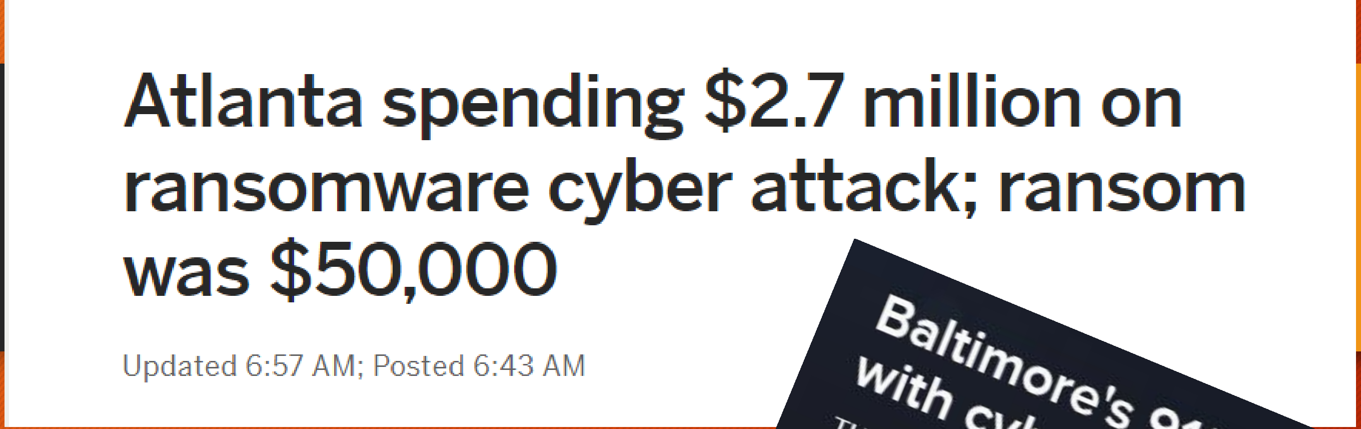
Cybersecurity is everyone's problem

- Cybersecurity is NOT just IT's problem.
  - IT
  - Emergency Management
  - Law Enforcement
  - And everyone in your organization



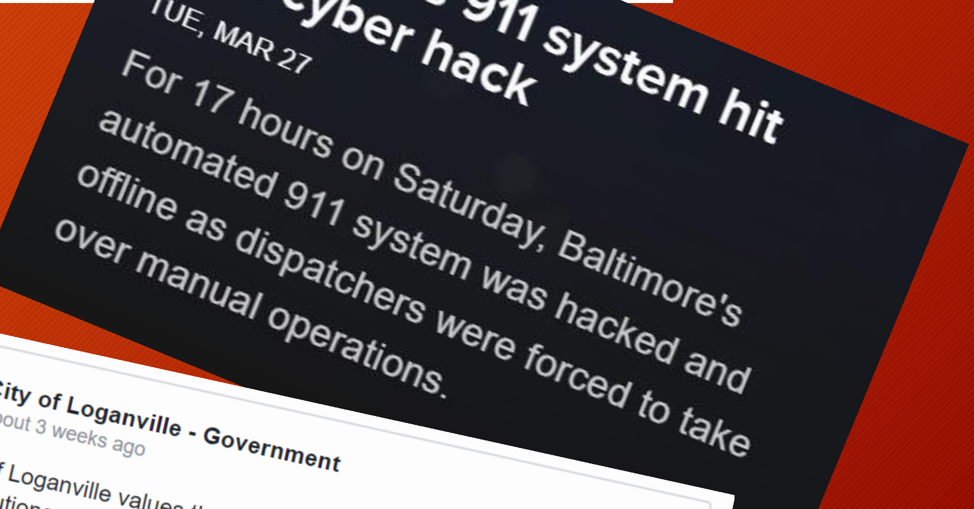
The threat

- Malicious vs unintentional
- Active attacks
- Data breaches
- Human error
- Cyber warfare



Atlanta spending $2.7 million on ransomware cyber attack; ransom was $50,000

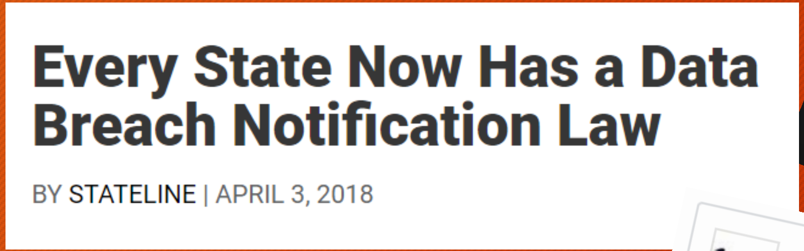
Updated 6:57 AM; Posted 6:43 AM



Baltimore's 911 system hit with cyber hack

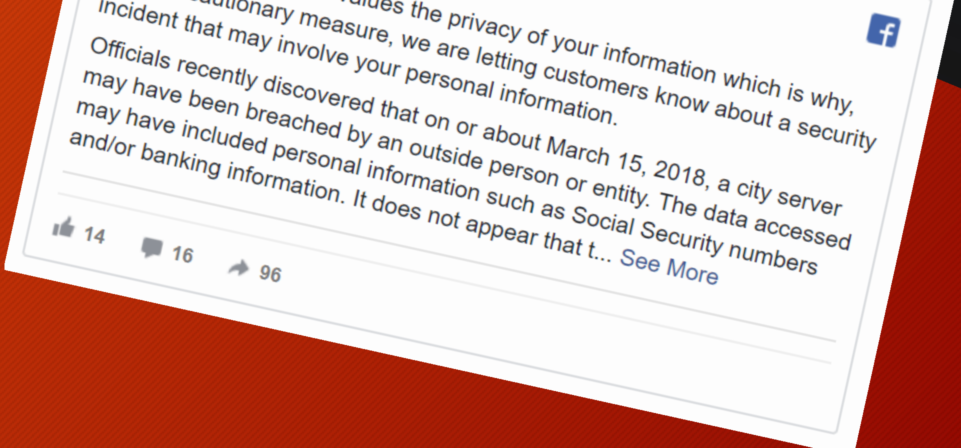
TUE, MAR 27

For 17 hours on Saturday, Baltimore's automated 911 system was hacked and offline as dispatchers were forced to take over manual operations.



Every State Now Has a Data Breach Notification Law

BY STATELINE | APRIL 3, 2018

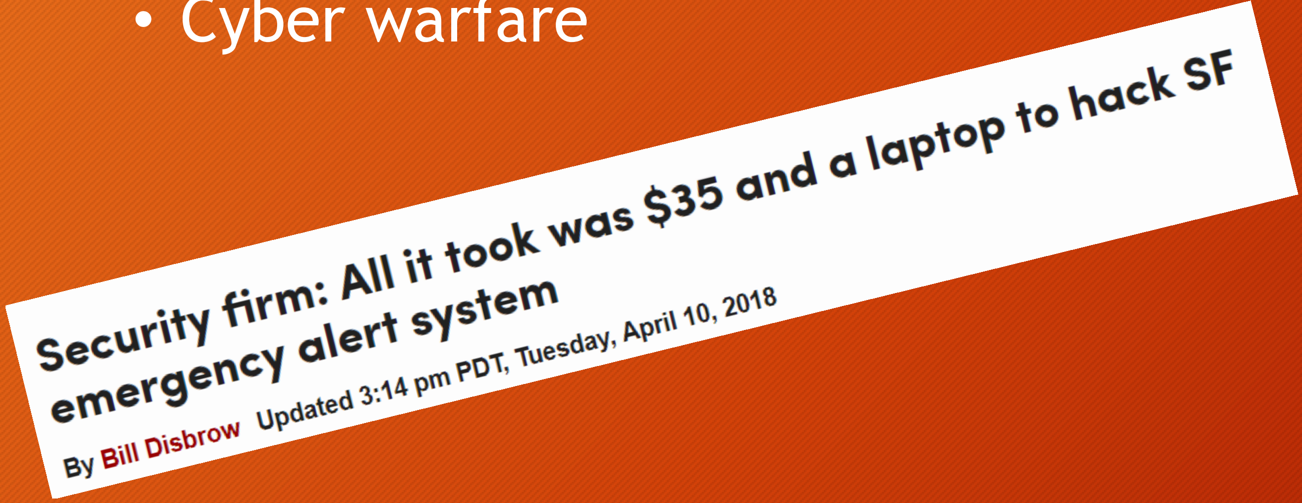


City of Loganville - Government

about 3 weeks ago

The City of Loganville values the privacy of your information which is why, as a precautionary measure, we are letting customers know about a security incident that may involve your personal information.

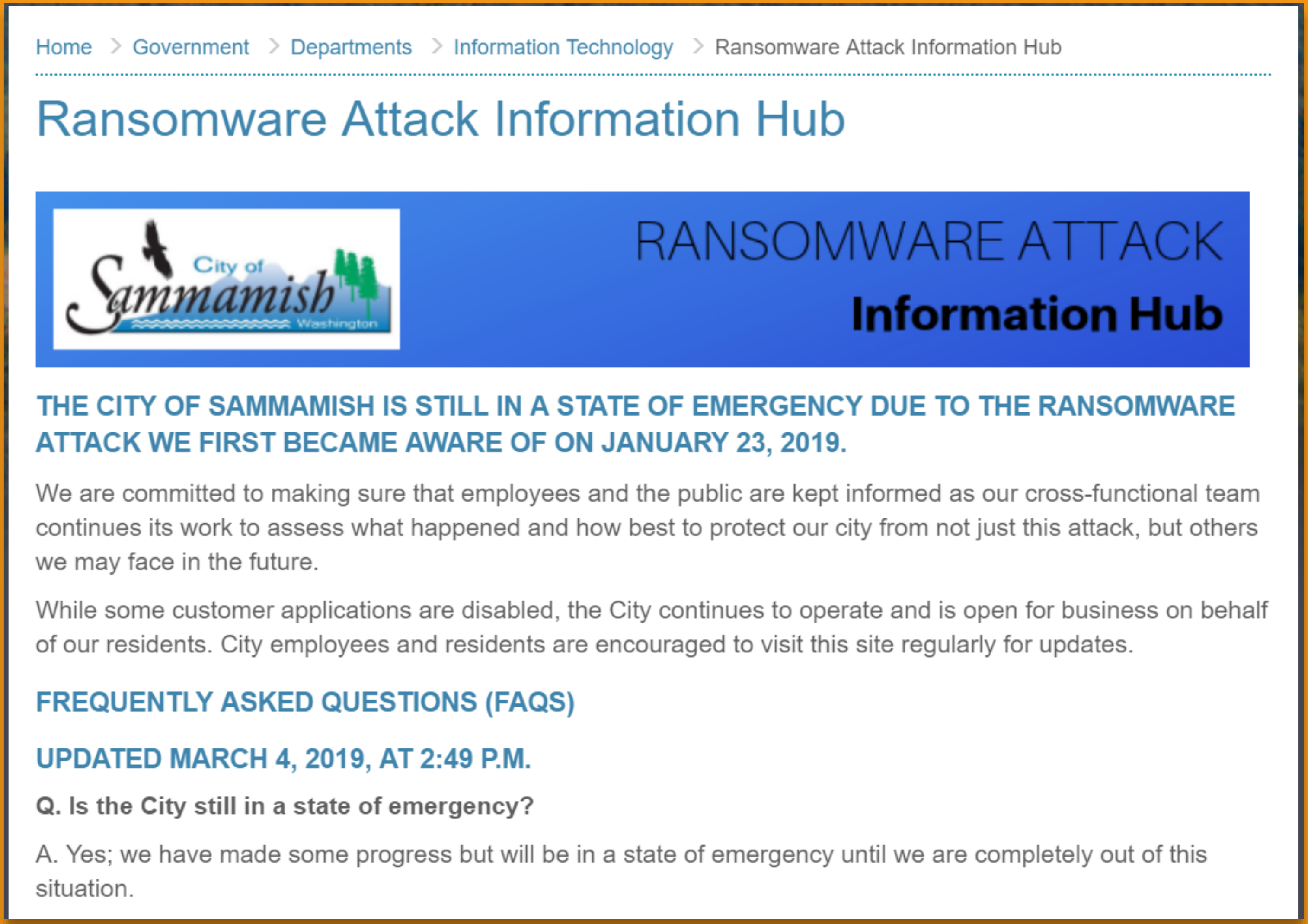
Officials recently discovered that on or about March 15, 2018, a city server may have been breached by an outside person or entity. The data accessed may have included personal information such as Social Security numbers and/or banking information. It does not appear that t... See More



Security firm: All it took was $35 and a laptop to hack SF emergency alert system

By Bill Disbrow Updated 3:14 pm PDT, Tuesday, April 10, 2018

Recently



Home > Government > Departments > Information Technology > Ransomware Attack Information Hub

Ransomware Attack Information Hub

City of Sammamish Washington

RANSOMWARE ATTACK

Information Hub

THE CITY OF SAMMAMISH IS STILL IN A STATE OF EMERGENCY DUE TO THE RANSOMWARE ATTACK WE FIRST BECAME AWARE OF ON JANUARY 23, 2019.

We are committed to making sure that employees and the public are kept informed as our cross-functional team continues its work to assess what happened and how best to protect our city from not just this attack, but others we may face in the future.

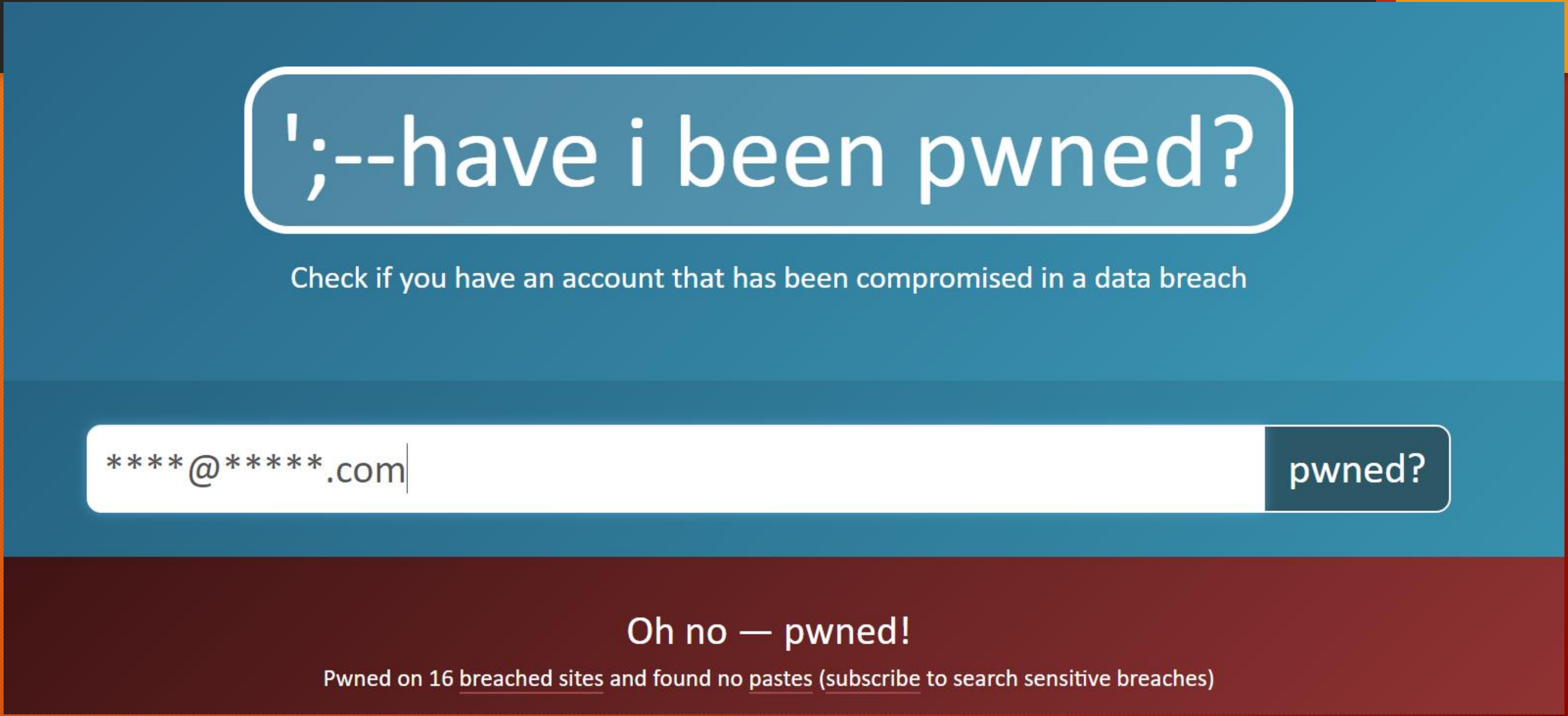
While some customer applications are disabled, the City continues to operate and is open for business on behalf of our residents. City employees and residents are encouraged to visit this site regularly for updates.

FREQUENTLY ASKED QUESTIONS (FAQS)

UPDATED MARCH 4, 2019, AT 2:49 P.M.

Q. Is the City still in a state of emergency?

A. Yes; we have made some progress but will be in a state of emergency until we are completely out of this situation.



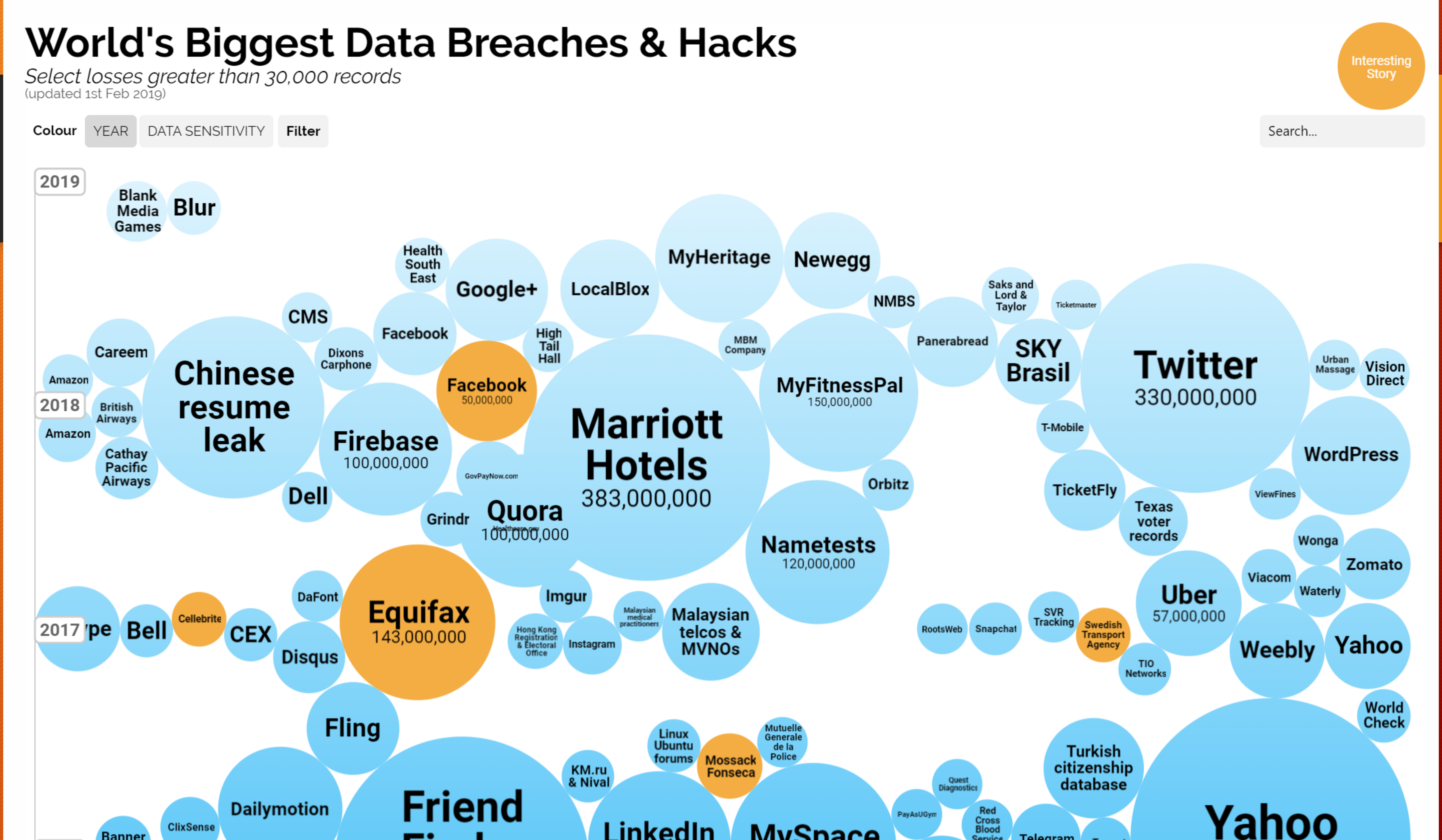
';--have i been pwned?

Check if you have an account that has been compromised in a data breach

****@*****.com

Oh no — pwned!

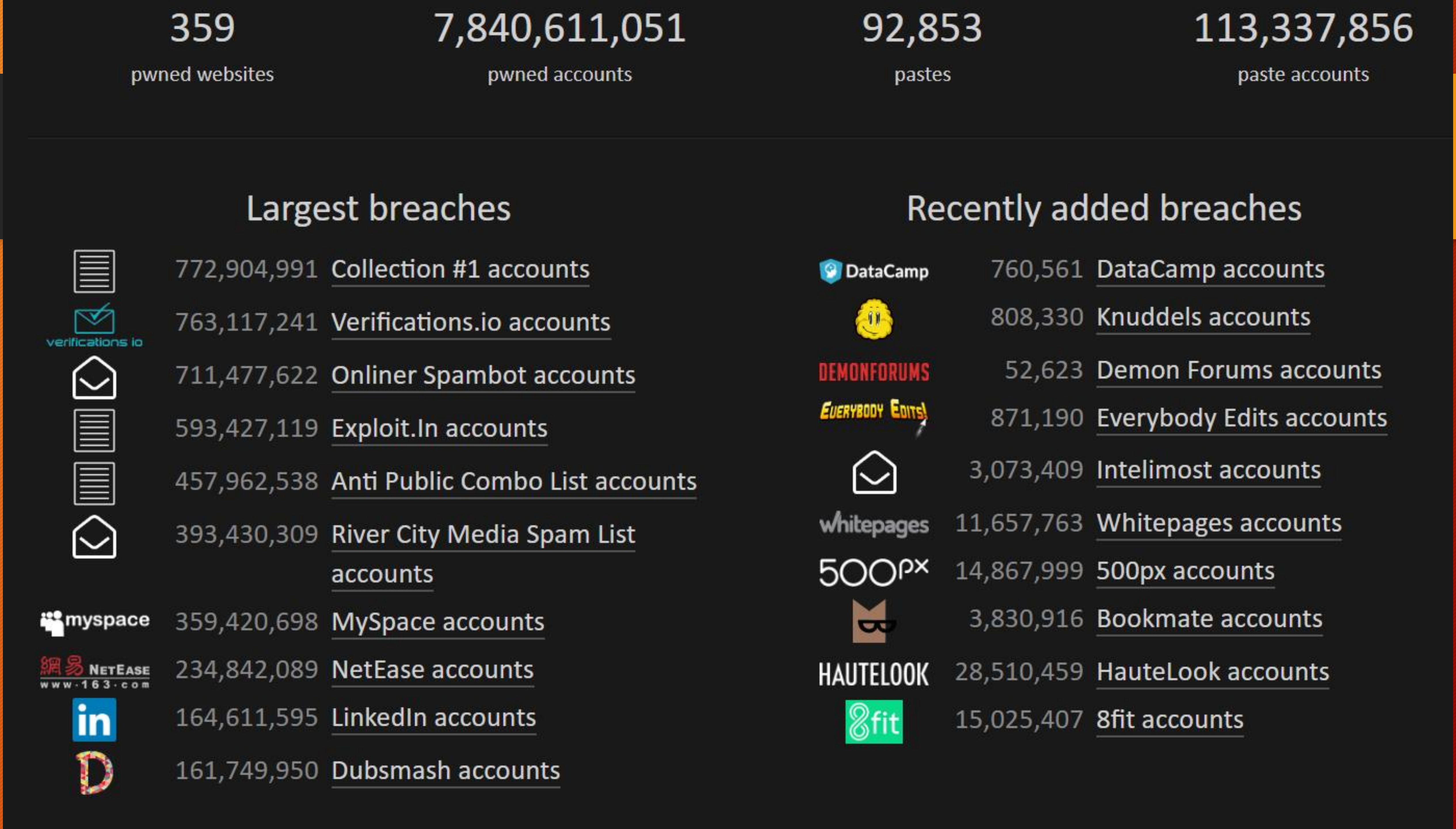
Pwned on 16 breached sites and found no pastes (subscribe to search sensitive breaches)



World's Biggest Data Breaches & Hacks

Select losses greater than 30,000 records

(updated 1st Feb 2019)



359	7,840,611,051	92,853	113,337,856
pwned websites	pwned accounts	pastes	paste accounts

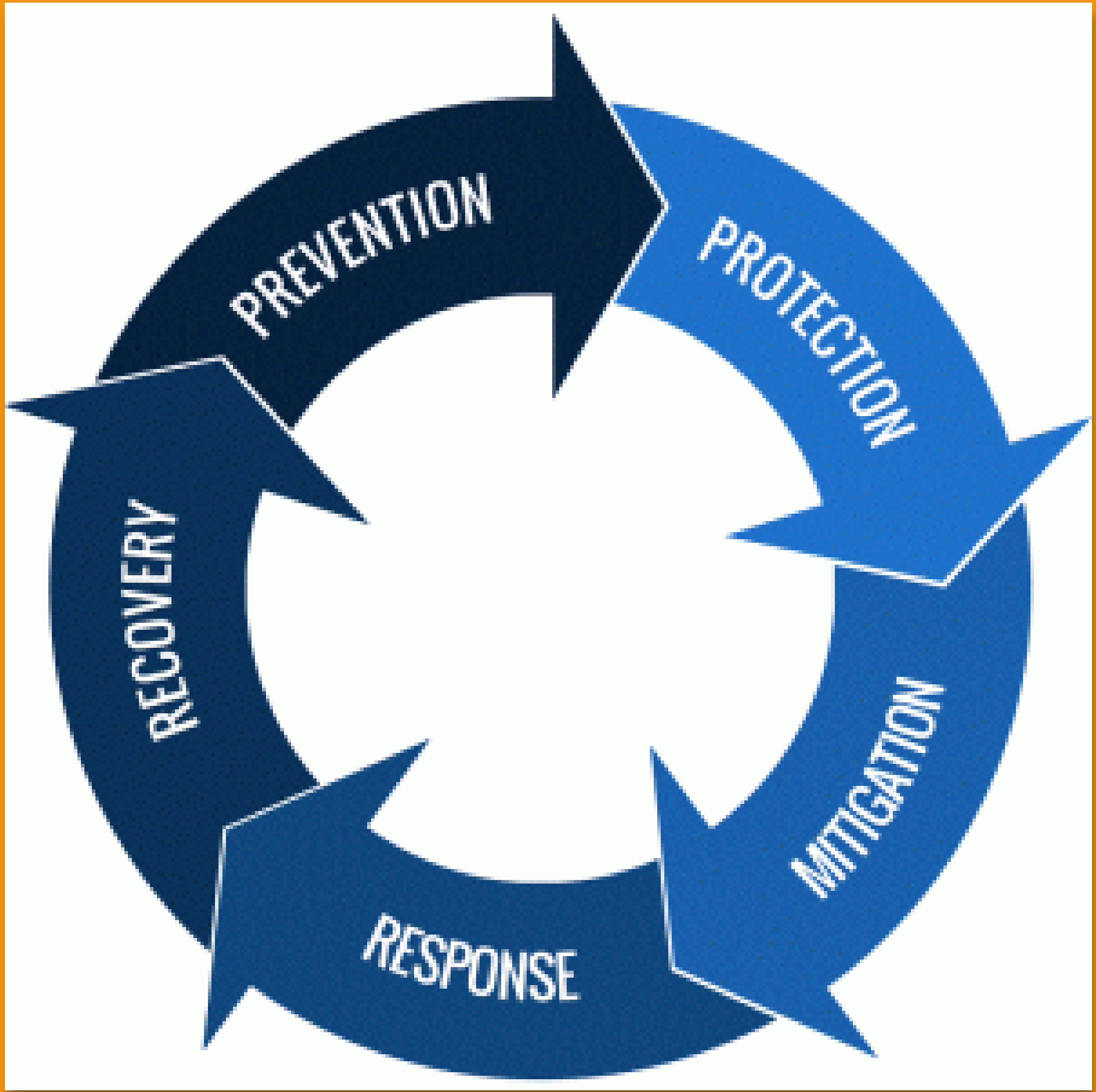
Largest breaches

772,904,991	Collection #1 accounts
763,117,241	Verifications.io accounts
711,477,622	Onliner Spambot accounts
593,427,119	Exploit.In accounts
457,962,538	Anti Public Combo List accounts
393,430,309	River City Media Spam List accounts
359,420,698	MySpace accounts
234,842,089	NetEase accounts
164,611,595	LinkedIn accounts
161,749,950	Dubsmash accounts

Recently added breaches

760,561	DataCamp accounts
808,330	Knuddels accounts
52,623	Demon Forums accounts
871,190	Everybody Edits accounts
3,073,409	Intelimost accounts
11,657,763	Whitepages accounts
14,867,999	500px accounts
3,830,916	Bookmate accounts
28,510,459	HauteLook accounts
15,025,407	8fit accounts

Lifecycle



Prevention

- What have you done to prepare?
- What policies are in place?
- What training is in place?
- How are the policies enforced?

- THINGS YOU MUST HAVE
- Emergency Operations Plan
- Cybersecurity Policy
- Acceptable Use Policy

Password Managers

wirecutter

A New York Times Company

Electronics › Storage

The Best Password Managers

https://thewirecutter.com/reviews/best-password-managers/

Protection

Mitigation

- What steps have you taken?
- What steps can you take?

- Insurance
- Backups
- Redundancy
- Monitoring
  - https://haveibeenpwned.com
- Early Reporting
- Training

Response

- Do you have a response plan?
- Does everybody know how to recognize an incident?
- Does your staff know what to do if they suspect an incident?
- Who do you call for help?

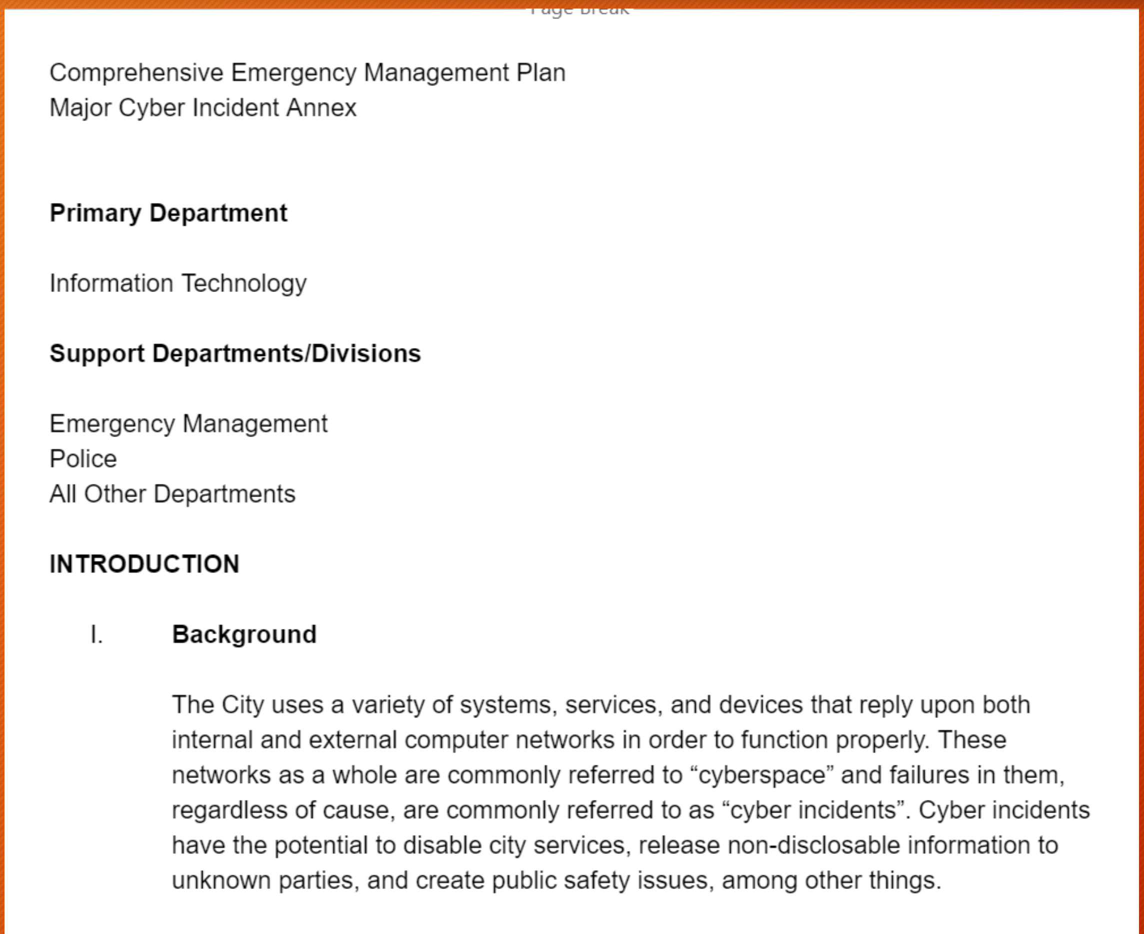
Recovery

What’s your recovery plan?

Beyond just the technology

Who do you call for help?

Sample Incident annex



Comprehensive Emergency Management Plan
Major Cyber Incident Annex

Primary Department

Information Technology

Support Departments/Divisions

Emergency Management
Police
All Other Departments

INTRODUCTION

I. **Background**

The City uses a variety of systems, services, and devices that reply upon both internal and external computer networks in order to function properly. These networks as a whole are commonly referred to "cyberspace" and failures in them, regardless of cause, are commonly referred to as "cyber incidents". Cyber incidents have the potential to disable city services, release non-disclosable information to unknown parties, and create public safety issues, among other things.

https://1drv.ms/w/s!At2Gwcs7z-oh3Ubt7QNXAZ-HHeM2

References

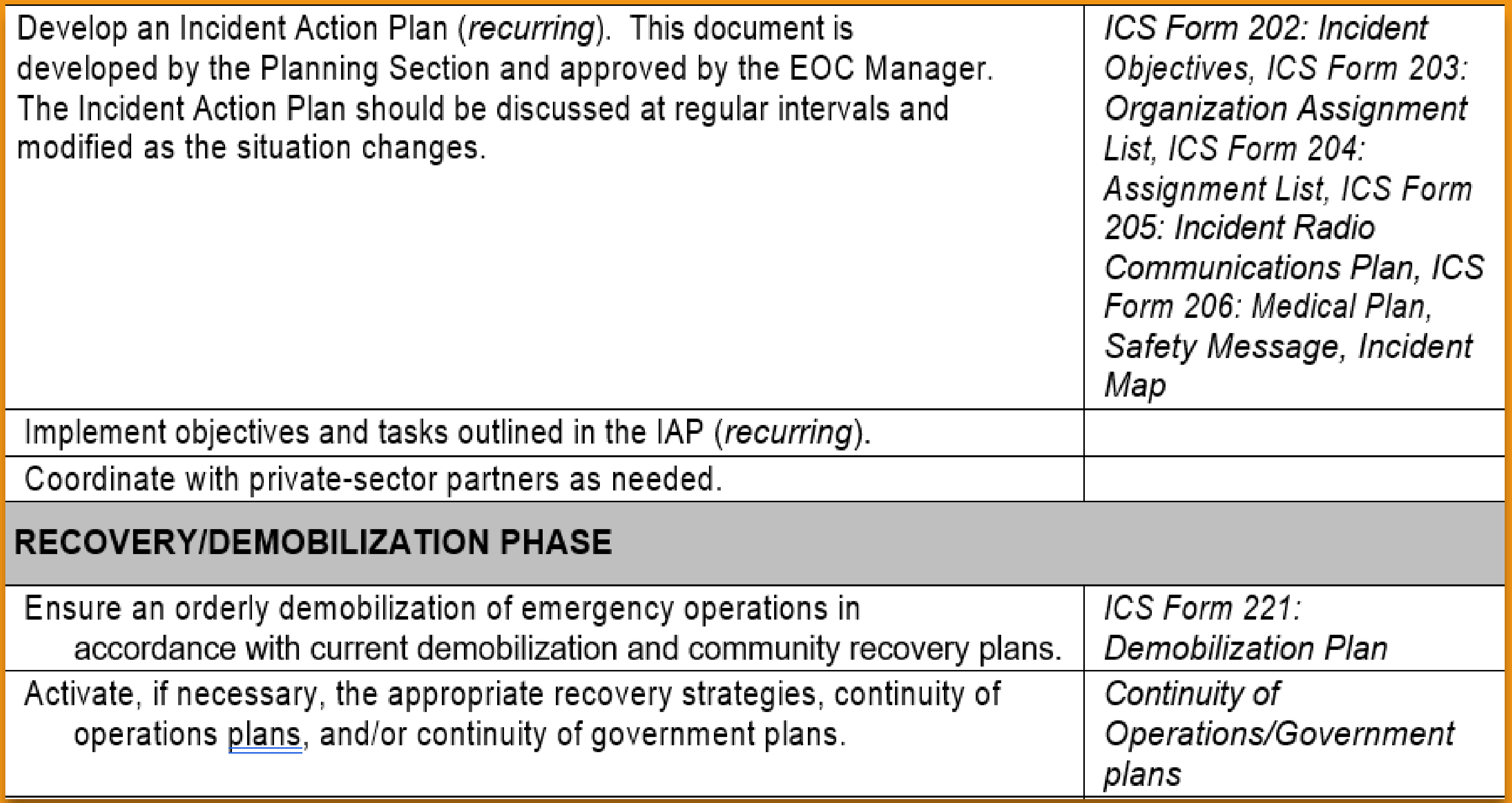
- National Cyber Incident Response Plan, Department of Homeland Security, 2016
- Computer Security Incident Handling Guide (Revision 2) National Institute of Standards and Technology, 2012
- Washington State Significant Cyber Incident Annex, Washington Military Department – Emergency Management Division, 2015
- ISO/IEC 27032 – Information Technology – Security techniques – Guidelines for cybersecurity, International Standards Organization, 2012

Annex Parts

Policies	Sets expectations
Situation/ Assumptions	Requires all components to be in place
Concept of Operations	Will require local discussion
Responsibilities	EM/IT/LE Expect some pushback

Major Cyber Incident Checklist

- Action items
  - Pre-Incident Phase
  - Response Phase
  - Recovery/Demob Phase



Develop an Incident Action Plan (*recurring*). This document is developed by the Planning Section and approved by the EOC Manager. The Incident Action Plan should be discussed at regular intervals and modified as the situation changes.	*ICS Form 202: Incident Objectives, ICS Form 203: Organization Assignment List, ICS Form 204: Assignment List, ICS Form 205: Incident Radio Communications Plan, ICS Form 206: Medical Plan, Safety Message, Incident Map*
Implement objectives and tasks outlined in the IAP (*recurring*).	
Coordinate with private-sector partners as needed.	
RECOVERY/DEMOBILIZATION PHASE	
Ensure an orderly demobilization of emergency operations in accordance with current demobilization and community recovery plans.	*ICS Form 221: Demobilization Plan*
Activate, if necessary, the appropriate recovery strategies, continuity of operations plans, and/or continuity of government plans.	*Continuity of Operations/Government plans*

Common Issues

- Most entities lack a comprehensive cybersecurity policy that vests responsibility with every employee.
- Those that have policies don’t enforce them
- A greater number of incidents occur than are reported in any formal way
- Lack of response plans leads to slow recognition, response, recovery.
- Lack of individual security leaves entire organization at risk

Human Factor

Phishing, social engineering

- Enabled by agency and employee use of social media and other things

Careless info access/dissemination

- Public spaces
- Public wifi
- Unlocked computers
- Lack of caution

Social Engineering

SOCIAL ENGINEERING

The clever manipulation of the natural human tendency to trust.

Social Media

- Names
- Personal details
- Personal details provided by third parties
- Account spoofing
- Operational details shared

Meet Desai

Meetkumar Hiteshbhai Desai

- Investigators traced the calls and discovered they originated from a link posted to Twitter and YouTube. The link was to a site named "Meet Desai" and its domain was hosted out of San Francisco. When the link was clicked, it continually called 911 and would not let the caller hang up.
- His page received 151,000 hits
- Desai said his intent was to make a non-harmful, yet annoying, bug that was meant to be funny, officials said.

- Surprise Police Department notified the Maricopa County Sheriff's Office of more than 100 hang-up 911 calls within a few minutes.
- The volume put authorities "in immediate danger of losing service to their switches."
- The emergency systems for the nearby Peoria Police Department and the Maricopa County Sheriff's Office also received a large number of repeated calls.
- Agencies in California and Texas were also affected.

It was not funny

OCTOBER 10, 2017

Meetkumar Desai, age 19, was sentenced to 3 years supervised probation for carrying out a reckless cyberattack on 911 emergency call systems in Maricopa County.

Authorities will also be able to monitor Desai’s computer while he is on probation.

Other Examples

This Photo by Unknown Author is licensed under CC BY-NC-SA

QUESTIONS?

Contact me:

Sarah Miller, MPA, CEM

President, IAEM Region 10

Past Chair, IAEM Emerging Tech Caucus

sarah@skmillerconsulting.com

twitter: @scba